



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,517	08/31/2000	Michael K. MacKay	7451.0029-00	4624
22852	7590	04/28/2005	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			CHEN, SHIN HON	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/653,517	MACKAY ET AL.	
Examiner	Art Unit		
Shin-Hon Chen	2131		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 04 January 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-20 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 31 August 2000 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____

DETAILED ACTION

1. Claims 1-20 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 2, 4-6, 8-10, 14, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis U.S. Pat. No. 6064739 (hereinafter Davis) in view of Grecsek U.S. Pat. No. 6088801 (hereinafter Grecsek).

4. As per claim 1, Davis discloses a method for protecting electronic content from unauthorized use by a user of a computer system, the method including: receiving a request from a user of the computer system to access a piece of electronic content and encapsulates encrypted digital data from the time it is received until it is provided to a display device to prevent software probing (Davis: column 1 lines 14-21 and column 1 lines 50 – column 2 line 29). Davis does not explicitly disclose identifying one or more software modules responsible for processing the piece of electronic content; evaluating one or more predefined characteristics of the one or more software modules; denying the request to access the piece of electronic content if the one or more predefined characteristics fail to satisfy a set of predefined criteria. However, Grecsek discloses

evaluate the risks of executing software processes based on capability-based policy to prevent unauthorized invocations of services located on the user's computer in order to protect data from unauthorized use (Grecsek: column 1 line 19 – column 2 line 47 and column 3 lines 17-51). Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Grecsek within the system of Davis because it increases data protection by making sure the data is not being used by unauthorized software hidden in the computer system.

5. As per claim 2, Davis as modified discloses a method as in claim 1. Davis as modified further discloses the method including: using the predefined criteria to evaluate a predefined policy, and basing a decision to deny the request on the outcome of this evaluation (Grecsek: column 3 lines 35-63 and column 4 lines 21-36).

6. As per claim 4, Davis discloses a system for protecting electronic content by preventing software probing and monitoring software and hardware devices from unauthorized access (Davis: column 1 lines 14-21 and column 1 lines 50 – column 2 line 29 and column 7 lines 6-28). David does not explicitly disclose the system comprising: means for applying a cryptographic fingerprint to the electronic content; means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content; means for denying effective access to the electronic content based on an output of said means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content; means for generating an identifier associated with the electronic content; means for monitoring a predefined

system interface for data containing the identifier; means for preventing effective access to data containing the identifier via the predefined system interface. However, Grecsek discloses a system for protecting data from unauthorized access by evaluating the risks of executing software processes based on capability-based policy to prevent unauthorized invocation s of services located on the user's computer in order to protect data from unauthorized use (Grecsek: column 1 line 19 – column 2 line 47 and column 3 lines 17-51; Grecsek: column 4 lines 43-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Grecsek within the system of Davis because it increases data protection by making sure the data is not being used by unauthorized software hidden in the computer system.

7. As per claim 5, Davis discloses a method for protecting electronic content from unauthorized use, the method including: (a) receiving a request to access a piece of electronic content (Davis: column 2 lines 58 – column 3 line 6) and protect it from unauthorized access by other software/hardware probing (Davis: column 1 lines 14-21 and column 1 lines 50 – column 2 line 29 and column 7 lines 6-28). Davis does not explicitly disclose (b) generating a first identifier associated with the electronic content; (c) monitoring at least one system interface, the monitoring including: (1) receiving a piece of electronic data; (2) generating a second identifier associated with the piece of electronic data; (3) comparing the second identifier with the first identifier; (4) taking a predefined defensive action if the second identifier is related to the first identifier in a predefined manner. However, Grecsek discloses a method for protecting data from unauthorized access by evaluating the risks of executing software processes based on capability-

based policy to prevent unauthorized invocation s of services located on the user's computer in order to protect data from unauthorized use (Grecsek: column 1 line 19 – column 2 line 47 and column 3 lines 17 – column 4 line 20; column 4 lines 43-55). Same rationale applies here as above in rejecting claim 1.

8. As per claim 6, Davis as modified discloses a method as in claim 5. Davis as modified further discloses the method including: (a)(1) decrypting the electronic content (Davis: column 2 lines 16-29).

9. As per claim 8, Davis as modified discloses a method as in claim 5. Davis as modified does not explicitly disclose in which the first identifier comprises a predefined portion of the electronic content and in which the second identifier comprises a predefined portion of the piece of electronic data. However, Herzberg discloses these limitations (Herzberg: column 1 line 44 – column 2 line 35). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Herzberg within the combination of Davis-Grecsek because it is well known in the art to authenticate whether an object is authorized for access by comparing two values.

10. As per claim 9, Davis as modified discloses a method as in claim 5. Davis as modified further discloses in which the system interface comprises a file system interface to one or more device drivers (Grecsek: column 3 line 52 – column 4 line 20).

11. As per claim 10, Davis as modified discloses a method as in claim 5. Davis discloses re-encrypting/modifying the piece of electronic data when the data is stored in the buffer to prevent software probing (Davis: column 2 lines 16-29 and column 1 lines 50 – column 2 line 29 and column 7 lines 6-28).

12. As per claim 14, Davis as modified discloses a method as in claim 5. Davis as modified further discloses in which the predefined defensive action comprises preventing the transfer of at least a portion of the piece of electronic data to an output device via the system interface (Grecsek: column 3 line 64 – column 4 line20).

13. As per claim 16, Davis as modified discloses a method as in claim . Davis as modified further discloses in which the at least one system interface is selected using rules associated with the electronic content, the rules being operable to identify certain system interfaces to which the electronic content is not allowed to be sent (Grecsek: column 3 line 64 – column 4 line20).

14. As per claim 17, Davis as modified discloses a method as in claim 9. Davis as modified further discloses in which the one or more device drivers are selected from the group consisting of: video display driver, sound driver, SCSI driver, IDE driver, network driver, video capture driver, floppy disk driver, and scanner driver (Grecsek: column 3 line 64 – column 4 line 27).

15. Claims 3, 7, 15, 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Grecsek and further in view of Herzberg et al. U.S. Pat. No. 5745678 (hereinafter Herzberg).

16. As per claim 3, Davis as modified discloses a method as in claim 1. Davis as modified does not explicitly disclose in which evaluating one or more predefined characteristics of the one or more software modules includes computing the cryptographic hash of at least one of the one or more software modules. However, Herzberg disclose using cryptographic hash value to authenticate whether a software program is authorized (Herzberg: column 1 line 44 – column 2 line 35). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Herzberg within the combination of Davis-Grecsek because it is well known in the art to authenticate whether an object is authorized for access using cryptographic hash.

17. As per claim 7, Davis as modified discloses a method as in claim 5. Davis as modified does not explicitly disclose the first identifier comprises a hash of at least a portion of the electronic content, and in which the second identifier comprises a hash of at least a portion of the piece, of electronic data. However, Herzberg discloses these limitations (Herzberg: column 1 line 44 – column 2 line 35). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Herzberg within the combination of Davis-Grecsek because it is well known in the art to authenticate whether an object is authorized for access using cryptographic hash.

18. As per claim 15, Davis as modified discloses a method as in claim 5. Davis as modified further discloses comparing the identifier to determine whether the software is allowed to be executed (Grecsek: column 3 line64 – column 4 line6). Alternatively, Herzberg also discloses comparing the first and second identifiers (Herzberg: column 1 line 52 – column 2 line 35). It would have been obvious to one having ordinary skill in the art to combine the teachings of Herzberg within the combination of Davis-Grecsek because it increases the security of the system by authenticating the program to ensure it is authorized program through comparison.

19. As per claim 18, Davis as modified discloses a method as in claim 5, Davis as modified does not explicitly disclose the method comprising: (a)(1) inserting a cryptographic fingerprint into the piece of electronic content, the cryptographic fingerprint containing information relating to the request to access said piece of electronic content. However, Herzberg discloses that limitation (Herzberg: column 1 line 52 – column 3 line 35). Same rationale applies here as above in rejecting claim 7.

20. As per claim 19, Davis as modified discloses a method as in claim 18, Davis as modified further discloses in which inserting said cryptographic fingerprint into the piece of electronic content includes: (i) authenticating a fingerprinting engine using a cryptographic credential; (ii) using the fingerprinting engine to insert the cryptographic fingerprint into the piece of electronic content (Herzberg: column 1 line 52 – column 3 line 35).

21. As per claim 20, Davis as modified discloses a method as in claim 19. Davis as modified further discloses in which the fingerprinting engine is operable to authenticate a calling application using a cryptographic credential (Herzberg: column 1 line 52 – column 3 line 35).

22. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Grecsek and further in view of Ciacelli et al. U.S. Pat. No. 6236727 (hereinafter Ciacelli).

23. As per claim 11, Davis as modified discloses a method as in claim 10. Davis as modified does not explicitly disclose in which modifying at least a portion of the piece of electronic data includes scrambling at least a portion of the piece of electronic data. However, Ciacelli discloses scrambling portion of electronic data to protect copyright data (Ciacelli: column 2 lines 3-65). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Ciacelli within the combination of Davis-Grecsek because scrambling a digital data protects the data from being viewed or used by unauthorized parties.

24. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Grecsek and further in view of Shimada European Patent No. EP0915620 (hereinafter Shimada).

25. As per claim 12 and 13, Davis as modified discloses a method as in claim 5. Davis as modified does not explicitly disclose the predefined defensive action comprises adding noise/electronic watermark to at least a portion of the piece of electronic data. However,

Shimada discloses that limitation (Shimada: [0011]-[0017]). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shimada within the combination of Davis-Grecsek because buring noise and digital watermark into data prevents unauthorized copy of a recorded data by an recording/reproducing device.

Response to Arguments

26. Applicant's arguments filed on 1/4/05 have been fully considered but they are not persuasive.

Regarding claim 1, applicant argues that the Davis reference discloses a hardware-based data protection. However, the term hardware and software can be used interchangeably due to the fact that hardware and software requires interoperability to work. Also, Davis reference is relied upon to disclose data protection system, but the method of examining software processes before execution is disclosed by Grecsek reference. Additionally, Grecsek reference discloses checking software on the computer system and the purpose of the process is to protect computer system resources including data received. Therefore, applicant's argument is respectfully traversed.

Regarding claims 4 and 5, they present the same scope as claim 1. Therefore, they are rejected based on same rationale set forth in claim 1. Additionally, Grecsek discloses the use of cryptographic method can also be applied in determining whether the software can be executed.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

SDMI, "SDMI Portable Device Specification Part 1 Version 1.0" discloses checking whether a device or application is SDMI compliant before execution of the device/application based on information contained in the digital data indicating whether the data should be protected.

Benson et al. U.S. Pat. No. 5845281 discloses controlling usage of digital data after it has been transmitted to intended users and checking the data to see if there is any control data in embedded in the data intended to restrict the use of the digital data.

28. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100